IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

ERICA TIERNEY and ANDRIS STRAUTINS, individually and on behalf of all others similarly situated,	
Plaintiffs,	**Case No:**
v.	
ADVOCATE HEALTH AND HOSPITALS CORP., a/k/a/ ADVOCATE MEDICAL GROUP, an Illinois corporation,	**JURY TRIAL DEMANDED**
Defendant.	

CLASS ACTION COMPLAINT

Plaintiffs Erica Tierney and Andris Strautins (together, "Plaintiffs"), on behalf of themselves and all others similarly situated, by and through their attorneys, bring this action against Advocate Health and Hospitals Corp., a/k/a Advocate Medical Group ("Advocate" or "Defendant"), and hereby allege as follows:

NATURE OF THE CASE

1. This is a consumer class action lawsuit brought by Plaintiffs, individually and on behalf of all other similarly situated persons (*i.e.*, the Class Members), whose unencrypted personally identifiable information and personal health information—names, addresses, dates of birth, Social Security numbers, treating physician and/or departments for each individual, their medical diagnoses, medical record numbers, medical service codes, and health insurance information (collectively referred to as "PII/PHI")—entrusted to Advocate was stolen by a thief or thieves while in the possession, custody, and control of Advocate.

2. On or about July 15, 2013, four laptop computers containing the unencrypted PII/PHI of Plaintiffs and more than four million Class Members were taken from one of Advocate's offices in Park Ridge, Illinois (the "Data Breach").

3. Advocate flagrantly disregarded Plaintiffs' and the other Class Members' privacy rights by intentionally, willfully, recklessly and/or negligently failing to take the necessary precautions required to safeguard and protect their PII/PHI from unauthorized disclosure. Plaintiffs' and Class Members' PII/PHI was improperly handled and stored, was unencrypted, and not kept in accordance with applicable and appropriate cyber-security protocols, policies and procedures. As a result, Plaintiffs' and Class Members' PII/PHI was compromised and stolen.

4. Advocate's intentional, willful, reckless, and/or negligent disregard of Plaintiffs' and Class Members' rights directly and/or proximately caused a substantial unauthorized disclosure of Plaintiffs' and Class Members' PII/PHI. The improper use of PII/PHI by unauthorized third parties can result in an adverse impact on, among other things, a victim's credit rating and finances. The type of wrongful PII/PHI disclosure made by Advocate is the most harmful because it generally takes a significant amount of time for a victim to become aware of misuse of that PII/PHI.

5. On behalf of themselves and Class Members, Plaintiffs have standing to bring this lawsuit because they were damaged as a direct and/or proximate result of Advocate's wrongful actions and/or inaction and the resulting Data Breach.

6. Advocate's wrongful actions and/or inaction and the resulting Data Breach have placed Plaintiffs and Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[1] Indeed, Javelin Strategy & Research ("Javelin"), a leading

[1] According to the United States Government Accounting Office, the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities, such as when PII/PHI is used to

provider of quantitative and qualitative research, released a 2012 Identity Fraud Report (the "Javelin Report"), quantifying the impact of data breaches. According to the Javelin Report, individuals whose PII/PHI is subject to a reported data breach—such as the Data Breach at issue here—are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft. Moreover, there is a high likelihood that significant identity theft and/or identity fraud has not yet been discovered or reported and a high probability that criminals who may now possess Plaintiffs' and Class Members' PII/PHI have not yet used the information but will do so later, or re-sell it. Even without such loss, Plaintiffs and Class Members are entitled to relief and recovery, including statutory damages under federal statutory provisions as set forth herein.

7. Advocate's failure to safeguard and secure Plaintiffs' and Class Members' PII/PHI violated the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et. seq.* ("FCRA"). Advocate failed to adopt, implement, and/or maintain adequate procedures to protect such information and limit its dissemination to the permissible purposes under FCRA. In further violation of FCRA, Advocate failed to protect and wrongfully disseminated Plaintiffs' and Class Members' PII/PHI, which is "medical information" specifically defined in, and protected by, FCRA. As a direct and/or proximate result of Advocate's willful, reckless and/or grossly negligent violations of FCRA, an unauthorized third party (or parties) obtained Plaintiffs' and Class Members' PII/PHI for no permissible purpose under FCRA.

8. Advocate's wrongful actions and/or inaction also constitute common law negligence and common law invasion of privacy by public disclosure of private facts.

---

commit fraud or other crimes (credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services)).

9. Plaintiffs, on behalf of themselves and the Class Members, seek actual damages, economic damages, statutory damages, nominal damages, exemplary damages, injunctive relief, attorneys' fees, litigation expenses and costs of suit.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over Plaintiffs' FCRA claims pursuant to 28 U.S.C. § 1331 (federal question). This Court also has subject matter jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367. This Court has personal jurisdiction over Advocate because at all relevant times, Advocate conducted (and continues to conduct) substantial business in the Northern District of Illinois.

11. Venue is proper in the Northern District of Illinois pursuant to 28 U.S.C. §1391(b) and (c) because a substantial part, if not all, of the events giving rise to this action occurred in the Northern District of Illinois and Advocate resides, is located, can be found, and/or conducts substantial business in the Northern District of Illinois.

PARTIES

12. Plaintiff Erica Tierney ("Tierney") is an Illinois citizen residing in the Northern District of Illinois. Tierney was treated at one of Advocate's facilities in Illinois during the relevant time period. On August 28, 2013, Tierney was advised that her PII/PHI was on the stolen laptop computers.

13. Tierney's PII/PHI, which she entrusted to Advocate that Advocate failed to properly safeguard, was stolen from Advocate on or about July 15, 2013.

14. As a direct and/or proximate result of Advocate's wrongful actions and/or inaction and the resulting Data Breach, Tierney has suffered economic damages and other actual harm, including but not limited to emotional distress over learning of the theft of her PII/PHI.

Advocate's wrongful disclosure of and failure to safeguard Tierney's PII/PHI has also placed her at an imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud, and medical fraud.

15. Plaintiff Andris Strautins ("Strautins") is an Illinois citizen residing in the Northern District of Illinois. Strautins was treated at one of Advocate's facilities in Illinois during the relevant time period. On or about August 26, 2013, Strautins received a letter from Advocate advising him that his PII/PHI was on laptop computers that had been stolen from Advocate's offices in Park Ridge, Illinois.

16. Strautins' PII/PHI, which he entrusted to Advocate that Advocate failed to properly safeguard, was stolen from Advocate on or about July 15, 2013.

17. As a direct and/or proximate result of Advocate's wrongful actions and/or inaction and the resulting Data Breach, Strautins has suffered economic damages and other actual harm, including but not limited to anxiety over learning of the theft of his PII/PHI. Advocate's wrongful disclosure of and failure to safeguard Strautins' PII/PHI has also placed him at an imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud, and medical fraud.

18. Defendant Advocate Health and Hospitals Corp. a/k/a Advocate Medical Group is a network of affiliated doctors and hospitals that treat patients throughout Illinois, with its principal place of business in Downers Grove, Illinois.

BACKGROUND FACTS

19. In the regular course of its business, Advocate collects and maintains possession, custody, and control of a wide variety of Plaintiffs' and Class Members' personal and confidential information, including: names, addresses, dates of birth, Social Security numbers,

treating physician and/or departments for each individual, their medical diagnoses, medical record numbers, medical service codes, and health insurance information (collectively referred to as "PII/PHI").

20. Advocate stored Plaintiffs' and Class Members' PII/PHI, at a minimum, in an unencrypted format on four laptop computers.

21. The unmonitored room in Advocate's administrative offices in Park Ridge, Illinois, where the unsecured computers containing Plaintiffs' and Class Members' unencrypted PII/PHI were stored, had little or no security to prevent unauthorized access.

22. On or about July 15, 2013, the four laptop computers containing Plaintiffs' and Class Members' unencrypted PII/PHI were removed from Advocate's Park Ridge facility (the "Data Breach").

23. Advocate does not know the whereabouts of the four laptop computers.

24. According to Advocate, the laptops contain the unencrypted PII/PHI of approximately 4.03 million Class Members whose health care provider is part of Advocate Health Care.

25. Despite knowing of the data loss since at least July 15, 2013, Advocate did not formally notify Plaintiffs and Class Members of the Data Breach until it started sending out letters to affected Class Members on August 23, 2013—more than one month after the theft of the four laptop computers.

26. During the intervening period between the theft and the date the notification letters were sent to Plaintiffs and Class Members on August 23, 2013, their unencrypted PII/PHI could have been bought and sold several times on the robust international cyber black market while they had no chance whatsoever to take measures to protect their privacy.

27. Advocate's wrongful actions and/or inaction—to wit, failing to protect Plaintiffs' and Class Members' PII/PHI with which it was entrusted—directly and/or proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' unencrypted PII/PHI without their knowledge, authorization, and/or consent. As a further direct and/or proximate result of Advocate's wrongful actions and/or inaction, Plaintiffs and Class Members have suffered, and will continue to suffer, damages including, without limitation: (i) the untimely and/or inadequate notification of the Data Breach; (ii) improper disclosure of their PII/PHI; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (vii) anxiety and emotional distress; and (viii) rights they possess under FCRA—for which they are entitled to compensation.

28. Notwithstanding Advocate's wrongful actions and/or inaction, Advocate has offered a mere one year of credit monitoring services, which is insufficient, given the trove of unencrypted PII/PHI that has been taken and disseminated to the world.

29. As a result of Advocate's failure to properly safeguard and protect Plaintiffs' and Class Members' PII/PHI, including, *inter alia*, failing to encrypt their PII/PHI and storing their PII/PHI on portable electronic devices such as laptops, and violating standard industry practices and protocols for protecting PII/PHI, Plaintiffs' and Class Members' privacy has been invaded and their rights violated. Their compromised PII/PHI was private and sensitive in nature and was left inadequately protected and unencrypted by Advocate. Advocate's wrongful actions and/or

inaction and the resulting Data Breach have placed Plaintiffs and Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.

30. Identity theft occurs when a person's PII, such as the person's name, e-mail address, address, Social Security number, billing and shipping addresses, phone number and credit card information is used without his or her permission to commit fraud or other crimes.[2]

31. According to the Federal Trade Commission ("FTC"), "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[3] Furthermore, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute [PII]."[4]

32. The FTC estimates that the identities of as many as 9 million Americans are stolen each year. *Id.*

33. As a direct and/or proximate result of the Data Breach, Plaintiffs and Class Members will now be required to take the time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, placing "freezes" and "alerts" with the credit reporting agencies, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity. Because Plaintiffs' and

[2] *See* http://www.consumer.ftc.gov/features/feature-0014-identity-theft (last visited Aug. 29, 2013).

[3] *Protecting Consumer Privacy in an Era of Rapid Change* FTC Report (March 2012) (http://www.ftc.gov/os/2012/03/120326privacyreport.pdf) (last visited Aug. 29, 2013).

[4] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, *Preliminary FTC Staff Report*, 35–38 (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (last visited Aug. 29, 2013); *Comment of Center for Democracy & Technology*, cmt. #00469, at 3; *Comment of Statz, Inc.*, cmt. #00377, at 11–12.

Class Members' Social Security numbers were stolen and compromised, they also now face a significantly heightened risk of identity theft.

34. According to the FTC, identity theft is serious. "Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest."[5]

35. Theft of medical information, such as that included in the Data Breach here, is equally serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[6]

36. Identity thieves also use Social Security numbers to commit other types of fraud. The GAO found that identity thieves use PII/PHI to open financial accounts and payment card accounts and incur charges in a victim's name. This type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft, while in the meantime causing significant harm to the victim's credit rating and finances. Moreover, unlike other PII/PHI, Social Security numbers are incredibly difficult to change and their misuse can continue for years into the future.

37. Identity thieves also use Social Security numbers to commit other types of fraud, such as obtaining false identification cards, obtaining government benefits in the victim's name,

[5] *See* Federal Trade Commission, *Signs of Identity Theft*, http://www.consumer.ftc.gov/articles/0271-signs-identity-theft (last visited Aug. 29, 2013).

[6] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Aug. 29, 2013).

committing crimes and/or filing fraudulent tax returns on the victim's behalf to obtain fraudulent tax refunds. Identity thieves also obtain jobs using stolen Social Security numbers, rent houses and apartments, and/or obtain medical services in the victim's name. Identity thieves also have been known to give a victim's personal information to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record. The GAO states that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

38. The unauthorized disclosure of a person's Social Security number can be particularly damaging since Social Security numbers cannot be easily replaced like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently, as well as show that he has done all he can to fix the problems resulting from the misuse.[7] Thus, a person whose PII/PHI has been stolen cannot obtain a new Social Security number until the damage has already been done.

39. Obtaining a new Social Security number also is not an absolute prevention against identity theft. Government agencies, private businesses and credit reporting companies likely still have the person's records under the old number, so using a new number will not guarantee a fresh start. For some victims of identity theft, a new number may actually create new problems. Because prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of a credit history.

40. As a direct and/or proximate result of Advocate's wrongful actions and/or inaction and the Data Breach, the thieves and/or their customers now have Plaintiffs' and Class

[7]*See* Identity Theft and Your Social Security Number, SSA Publication No. 05-10064, October 2007, ICN 46327 (http://www.ssa.gov/pubs/10064.html) (last visited Aug. 29, 2013).

Members' PII/PHI. As such, Plaintiffs and Class Members have been deprived of the value of their PII/PHI.[8]

41. Plaintiffs' and Class Members' PII/PHI is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for a number of years.[9] Identity thieves and other cyber criminals openly post stolen credit card numbers, Social Security numbers, and other personal financial information on various Internet websites, thereby making the information publicly available. In one study, researchers found hundreds of websites displaying stolen personal financial information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism—the "Safe Browsing list." The study concluded:

> It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that the black market for cyber criminals is not underground at all. In fact, it's very "in your face."[10]

42. The Data Breach was a direct and/or proximate result of Advocate's failure to implement and maintain appropriate and reasonable security procedures and practices to safeguard and protect Plaintiffs' and Class Members' PII/PHI from unauthorized access, use, and/or disclosure, as required by various state regulations and industry practices.

---

[8] *See, e.g.*, John T. Soma, J. Zachary Courson, John Cadkin, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted); ABC News Report, http://abcnews.go.com/Health/medical-records-private-abc-news-investigation/story?id=17228986&page=2#.UGRgtq7yBR4 (last visited Aug. 29, 2013).

[9] Companies, in fact, also recognize PII/PHI as an extremely valuable commodity akin to a form of personal property. *See* T. Soma, *et al*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009).

[10] StopTheHacker, *The "Underground Credit Card Blackmarket*, http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/ (last visited Aug. 29, 2013).

43. Advocate flagrantly disregarded and/or violated Plaintiffs' and Class Members' privacy rights, and harmed them in the process, by not obtaining Plaintiffs' and Class Members' prior written consent to disclose their PII/PHI to any other person—as required by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and other pertinent laws, regulations, industry standards and/or internal company standards.

44. Advocate flagrantly disregarded and/or violated Plaintiffs' and Class Members' privacy rights, and harmed them in the process, by failing to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII/PHI to protect against anticipated threats to the security or integrity of such information. Advocate's security deficiencies allowed unauthorized individuals to access, remove from its premises, transport, disclose, and/or compromise the PII/PHI of millions of individuals—including Plaintiffs and Class Members.

45. Advocate's wrongful actions and/or inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' PII/PHI without their knowledge, authorization, and consent. As a direct and proximate result of Advocate's wrongful actions and/or inaction and the resulting Data Breach, Plaintiffs and Class Members have incurred damages in the form of, *inter alia*: (i) the untimely and/or inadequate notification of the Data Breach; (ii) improper disclosure of their PII/PHI; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (vii) anxiety and emotional distress; and (viii) rights they possess under

FCRA—for which they are entitled to compensation.

CLASS ACTION ALLEGATIONS

46. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this class action as a national class action on behalf of themselves and the following Class of similarly situated individuals:

> All persons whose unencrypted personal identifying information (PII) and personal health information (PHI) were contained on the laptop computers reported stolen from the Advocate Medical Group administrative offices in Park Ridge, Illinois on or about July 15, 2013.

Excluded from the Class are the (i) owners, officers, directors, employees, agents and/or representatives of Defendant and its parent entities, subsidiaries, affiliates, successors, and/or or assigns, and (iii) the Court, Court personnel, and members of their immediate families.

47. The putative Class is comprised of over four million persons, making joinder impracticable. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the Parties and the Court.

48. The rights of each Class Member were violated in a virtually identical manner as a result of Advocate's willful, reckless, and/or negligent actions and/or inaction.

49. Questions of law and fact common to all Class Members exist and predominate over any questions affecting only individual Class Members including, *inter alia*:

a) Whether Advocate violated FCRA by failing to properly secure Plaintiffs' and Class Members' PII/PHI;

b) Whether Advocate violated FCRA by failing to encrypt Plaintiffs' and Class Members' PII/PHI in accordance with federal standards;

c) Whether Advocate willfully, recklessly, and/or negligently failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class Members' PII/PHI;

d) Whether Advocate was negligent in storing Plaintiffs' and Class Members' PII/PHI;

e) Whether Advocate owed a duty to Plaintiffs and Class Members to exercise reasonable care in protecting and securing their PII/PHI;

f) Whether Advocate breached its duty to exercise reasonable care in protecting and securing Plaintiffs' and Class Members' PII/PHI;

g) Whether Advocate was negligent in failing to secure Plaintiffs' and Class Members' PII/PHI;

h) Whether by publicly disclosing Plaintiffs' and Class Members' PII/PHI without authorization, Advocate invaded Plaintiffs' and Class Members' privacy;

i) Whether Plaintiffs and Class Members sustained damages as a result of Advocate's failure to secure and protect their PII/PHI; and

j) Whether Advocate violated federal and/or state laws by failing to timely notify Plaintiffs and Class Members on an individual basis about the theft and dissemination of their PII/PHI.

50. Plaintiffs' claims are typical of Class Members' claims in that Plaintiffs' claims and Class Members' claims all arise from Advocate's failure to properly secure and protect Plaintiffs' and Class Members' PII/PHI and the resulting data breach.

51. Plaintiffs and their counsel will fairly and adequately represent the interests of Class Members. Plaintiffs have no interests antagonistic to, or in conflict with, Class Members' interests. Plaintiffs' lawyers are highly experienced in the prosecution of consumer class actions and data breach class actions, and intend to vigorously prosecute this action on behalf of Plaintiffs and Class Members.

52. A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiffs' and Class Members' claims. Plaintiffs and Class Members have been irreparably harmed as a result of Advocate's wrongful actions and/or inaction. Litigating this

case as a class action will reduce the possibility of repetitious litigation relating to Advocate's failure to secure and protect Plaintiffs' and Class Members' PII/PHI.

53. Class certification, therefore, is appropriate pursuant to FED. R. CIV. P. 23(b)(3) because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

54. Class certification also is appropriate pursuant to FED. R. CIV. P. 23(b)(2) because Defendant have acted or refused to act on grounds generally applicable to the class, thereby making final injunctive relief appropriate with respect to the patients of the class as a whole.

55. The expense and burden of litigation would substantially impair the ability of Class Members to pursue individual lawsuits in order to vindicate their rights.

CLAIMS FOR RELIEF/CAUSES OF ACTION

COUNT I
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT

56. The preceding factual statements and allegations are incorporated by reference.

57. FCRA requires consumer reporting agencies to adopt and maintain procedures for meeting the needs of commerce for consumer credit, personnel, insurance and other information in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information. 15 U.S.C. § 1681(b).

58. FCRA defines a "consumer reporting agency" as:

> Any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

15 U.S.C. § 1681a(f).

59. FCRA defines a "consumer report" as:

> [A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes, or any other purpose authorized under [15 U.S.C. §] 1681(b).

15 U.S.C. § 1681a(d)(1).

60. FCRA defines "medical information" as:

> [I]nformation or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to--(A) the past, present, or future physical, mental, or behavioral health or condition of an individual; (B) the provision of health care to an individual; or (C) the payment for the provision of health care to an individual.

15 U.S.C. § 1681a(i).

61. FCRA specifically protects medical information, restricting its dissemination to limited instances. *See, e.g.,* 15 U.S.C. §§ 1681a(d)(3); 1681b(g); 1681c(a)(6).

62. Advocate is a Consumer Reporting Agency as defined under FCRA because on a cooperative nonprofit basis and/or for monetary fees, Advocate regularly engages, in whole or in part, in the practice of assembling information on consumers for the purpose of furnishing Consumer Reports to third parties and/or uses interstate commerce for the purpose of preparing and/or furnishing Consumer Reports.

63. As a Consumer Reporting Agency, Advocate was (and continues to be) required to adopt and maintain procedures designed to protect and limit the dissemination of consumer

credit, personnel, insurance and other information (such as Plaintiffs' and Class Members' PII/PHI) in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information. Advocate, however, violated FCRA by failing to adopt and maintain such protective procedures which, in turn, directly and/or proximately resulted in the theft of laptop computers containing Plaintiffs' and Class Members' unencrypted PII/PHI and its wrongful dissemination into the public domain. In addition to encrypting Plaintiffs' and Class Members' PII/PHI, Advocate could have:

a) Conducted periodic risk assessments and gap analysis relating to privacy and information security-related policies, processes and procedures. A comprehensive risk analysis would have identified the (i) physical vulnerability of Advocate's locations, (ii) administrative vulnerabilities associated with storing over four million patient records on four laptop computers, and (iii) technical vulnerabilities, including the need to restrict unauthorized access and encrypt at-risk data.

b) Developed privacy and information security related performance and activity metrics, such as the performance of ongoing compliance reviews, physical walkthroughs (roundings), hotline and complaint management—and ensure that these metrics were an integral part of Advocate's corporate governance program.

c) Taken measures to monitor and secure the room and areas where the laptop computers containing the PII/PHI were stored, maintained, and used, or taken measures to insure that no PII/PHI was stored on portable, unencrypted electronic devices.

On information and belief, Advocate took none of these proactive actions to secure and protect Plaintiffs' and Class Members' PII/PHI and/or put itself in a position to immediately notify Plaintiffs and Class Members about the data breach.

64. Plaintiffs' and Class Members' PII/PHI, in whole or in part, constitutes medical information as defined by FCRA. Advocate violated FCRA by failing to specifically protect and

limit the dissemination of Plaintiffs' and Class Members' PII/PHI (*i.e.*, their medical information) into the public domain.

65. As a direct and/or proximate result of Advocate's willful and/or reckless violations of FCRA, as described above, Plaintiffs' and Class Members' unencrypted PII/PHI was stolen and made accessible to unauthorized third parties in the public domain.

66. As a direct and/or proximate result of Advocate's willful and/or reckless violations of FCRA, as described above, Plaintiffs and Class Members were (and continue to be) damaged in the form of, without limitation, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy and other economic and non-economic harm.

67. Plaintiffs and Class Members, therefore, are entitled to compensation for their actual damages including, *inter alia*, (i) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (ii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iii) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (iv) anxiety and emotional distress; and (v) statutory damages of not less than $100, and not more than $1000, each, as well as attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. §1681n(a).

COUNT II
NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT

68. The factual statements and allegations in paragraphs 1–55 of this Complaint are incorporated by reference.

69. In the alternative, and as described above, Advocate negligently violated FCRA by failing to adopt and maintain procedures designed to protect and limit the dissemination of

Plaintiffs' and Class Members' PII/PHI for the permissible purposes outlined by FCRA which, in turn, directly and/or proximately resulted in the theft of a laptop computer and wrongful dissemination of Plaintiffs' and Class Members' PII/PHI into the public domain. In addition to encrypting Plaintiffs' and Class Members' PII/PHI, Advocate could have:

a) Conducted periodic risk assessments and gap analysis relating to privacy and information security-related policies, processes and procedures. A comprehensive risk analysis would have identified the (i) physical vulnerability of Advocate's locations, (ii) administrative vulnerabilities associated with storing over four million patient records on four laptop computers, and (iii) technical vulnerabilities, including the need to restrict unauthorized access and encrypt at-risk data.

b) Developed privacy and information security related performance and activity metrics, such as the performance of ongoing compliance reviews, physical walkthroughs (roundings), hotline and complaint management—and ensure that these metrics were an integral part of Advocate's corporate governance program.

c) Taken measures to monitor and secure the room and areas where the laptop computers containing the PII/PHI were stored, maintained, and used, or taken measures to insure that no PII/PHI was stored on portable, unencrypted electronic devices.

On information and belief, Advocate took none of these proactive actions to secure and protect Plaintiffs' and Class Members' PII/PHI and/or put itself in a position to immediately notify Plaintiffs and Class Members about the Data Breach.

70. It was reasonably foreseeable that Advocate's failure to implement and maintain procedures to protect and secure Plaintiffs' and Class Members' PII/PHI would result in an unauthorized third party gaining access to their PII/PHI for no permissible purpose under FCRA.

71. As a direct and/or proximate result of Advocate's negligent violations of FCRA, as described above, Plaintiffs' and Class Members' PII/PHI was stolen and made accessible to unauthorized third parties in the public domain.

72. As a direct and/or proximate result of Advocate's negligent violations of FCRA, as described above, Plaintiffs and the Class Members were (and continue to be) damaged in the form of, without limitation, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

73. Plaintiffs and Class Members, therefore, are entitled to compensation for their actual damages, including, *inter alia*: (i) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (ii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iii) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (iv) anxiety and emotional distress; and (viii) attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. §1681o(a).

COUNT III
NEGLIGENCE

74. The factual statements and allegations in paragraphs 1–55 of this Complaint are incorporated by reference.

75. Advocate had a duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII/PHI.

76. Advocate violated its duty by failing to exercise reasonable care and safeguard and protect Plaintiffs' and Class Members' PII/PHI (as set forth in detail above).

77. It was reasonably foreseeable that Advocate's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII/PHI would result in an unauthorized third party gaining access to such information for no lawful purpose.

78. Plaintiffs and the Class Members were (and continue to be) damaged as a direct and/or proximate result of Advocate's failure to secure and protect their PII/PHI in the form of, *inter alia*, (i) improper disclosure of their PII/PHI; (ii) loss of privacy; (iii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (iv) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (vi) anxiety and emotional distress— for which they are entitled to compensation.

79. Advocate's wrongful actions and/or inaction (as described above) constituted negligence at common law.

COUNT IV
INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS

80. The factual statements and allegations in paragraphs 1–55 of this Complaint are incorporated herein by reference.

81. Advocate's failure to secure and protect Plaintiffs' and Class Members' PII/PHI directly resulted in the public disclosure of such private information.

82. Dissemination of Plaintiffs' and Class Members' PII/PHI is not of a legitimate public concern; publicity of their PII/PHI would be, is and will continue to be offensive to reasonable people.

83. Plaintiffs and the Class Members were (and continue to be) damaged as a direct and/or proximate result of Advocate's invasion of their privacy by publicly disclosing their private facts (*i.e.*, their PII/PHI) in the form of, *inter alia*: (i) improper disclosure of their PII/PHI; (ii) loss of privacy; (iii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (iv) the value of

their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (vi) anxiety and emotional distress— for which they are entitled to compensation. At the very least, Plaintiffs and the Class Members are entitled to nominal damages.

84. Advocate's wrongful actions and/or inaction (as described above) constituted (and continue to constitute) an ongoing invasion of Plaintiffs' and Class Members' privacy by publicly disclosing their private facts (*i.e.*, their PII/PHI).

RELIEF REQUESTED

85. The preceding factual statements and allegations are incorporated herein by reference.

86. **DAMAGES.** As a direct and/or proximate result of Advocate's wrongful actions and/or inaction (as described above), Plaintiffs and Class Members suffered (and continue to suffer) damages in the form of, *inter alia*: (i) the untimely and/or inadequate notification of the Data Breach; (ii) improper disclosure of their PII/PHI; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (vii) anxiety and emotional distress; and (viii) rights they possess under FCRA—for which they are entitled to compensation. Plaintiffs and Class Members also are entitled to recover statutory damages and/or nominal damages. Plaintiffs' and Class Members' damages were foreseeable by Advocate and exceed the minimum jurisdictional limits of this Court.

87. **EXEMPLARY DAMAGES.** Plaintiffs and Class Members also are entitled to exemplary damages as punishment and to deter such wrongful conduct in the future.

88. **INJUNCTIVE RELIEF.** Plaintiffs and Class Members also are entitled to injunctive relief in the form of, without limitation, requiring Advocate to, *inter alia*, (i) immediately disclose to Plaintiffs and Class Members the precise nature and extent of their PII/PHI contained on the stolen laptop computers, (ii) make prompt and detailed disclosure to all past, present and future patients affected by any future data breaches of their PII/PHI, (iii) immediately encrypt the PII/PHI of its past, present, and future patients, (iv) implement the above-referenced proactive policies and procedures in order to secure and protect its patients' PII/PHI and be in a position to immediately notify them about any data breaches, (v) submit to periodic compliance audits by a third party regarding the implementation of and compliance with such policies and procedures, and (vi) submit to periodic compliance audits by a third party regarding the security of its patients' PII/PHI within its possession, custody and control.

89. **ATTORNEYS' FEES, LITIGATION EXPENSES AND COSTS.** Plaintiffs and Class Members also are entitled to recover their attorneys' fees, litigation expenses and court costs in prosecuting this action pursuant to, *inter alia,* 15 U.S.C. §§ 1681n(a); o(a).

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, respectfully requests that (i) Advocate be cited to appear and answer this lawsuit, (ii) this action be certified as a class action, (iii) Plaintiffs be designated the Class Representatives, and (iv) Plaintiffs' counsel be appointed as Class Counsel. Plaintiffs, on behalf of themselves and Class Members, further request that upon final trial or hearing, judgment be awarded against Advocate, in favor of Plaintiffs and the Class Members, for:

(i) actual damages, consequential damages, FCRA statutory damages and/or nominal damages (as described above) in an amount to be determined by the trier of fact;

(ii) exemplary damages:

(iii) injunctive relief as set forth above;

(iv) pre- and post-judgment interest at the highest applicable legal rates;

(v) attorneys' fees and litigation expenses incurred through trial and any appeals;

(vi) costs of suit; and

(vii) such other and further relief that this Court deems just and proper.

JURY DEMAND

Plaintiffs, on behalf of themselves and all others similarly situated, respectfully demand a trial by jury on all of the claims and causes of action so triable.

Respectfully submitted,

/s/ Ben Barnow
Ben Barnow
Sharon Harris
Blake A. Strautins
BARNOW AND ASSOCIATES, P.C.
One N. LaSalle Street, Ste. 4600
Chicago, IL 60602
Telephone: (312) 621-2000
Facsimile: (312) 641-5504
Email: b.barnow@barnowlaw.com
Email: s.harris@barnowlaw.com
Email: b.strautins@barnowlaw.com

Aron D. Robinson
Law Office of Aron D. Robinson
180 West Washington St., Suite 700
Chicago, IL 60602
Telephone: (312) 857-9050
Email: Adroblaw@aol.com

Of Counsel:

Richard L. Coffman
THE COFFMAN LAW FIRM
First City Building
505 Orleans St., Ste. 505
Beaumont, TX 77701
Telephone: (409) 833-7700
Facsimile: (866) 835-8250
Email: rcoffman@coffmanlawfirm.com